Candidate Access Router Discovery

Päivi Kankaanpää
Helsinki University of Technology
Telecommunications software and multimedia laboratory

May 28, 2003

Abstract

Candidate access router discovery (CARD) is used to find the access routers the mobile node could connect to when leaving its current access router, and to discover the capabilities of the new access routers. To serve this purpose CARD has two functions: reverse address translation and discovery of candidate access router capabilities. CARD can be used in mobile node orchestrated mode or in network assisted mode. When the candidate access routers have been found and it is time to hand over to the new access router the target access router selection is executed. CARD is needed to make seamless handovers possible.

1 Introduction

The purpose of this document is to give an overview on candidate access router discovery (CARD). The discussion is based on Internet Drafts created in Internet Engineering Task Force’s (IETF’s) Seamoby Working Group.

In wireless networks mobile nodes need every now and then to change their access router (AR). To make this handover seamless there is a need to know in advance where to connect. Candidate access router discovery is used to find those access routers to which the mobile node (MN) could connect. All routers do not have equal capabilities and in order to be able to make a decision where the mobile node could get the service it needs, candidate access router discovery finds out candidate access routers’ capabilities.

Figure 1 illustrates the basic situation. The MN is connected to the current AR through the current access point (AP). The coverage areas of AP1 and AP2 also cover the MN’s current location. So, there are two candidate access routers (CARs) AR1 and AR2 serving the AP1 and AP2, respectively. CARD solves the IP addresses and the capabilities of the routers AR1 and AR2. The AR3 is not a CAR because the MN is not in the coverage area of AP3. The access points connect to their serving access routers. The access routers connect further to the IP network.

Some features that can be implemented with CARD are load balancing, least-cost calls and resource intensive applications. Based on the capability information the mobile node could choose the AR with least load and thus help in balancing the load between ARs, or
the new router could be chosen based on access prices to get the cheapest possible service. Resource intensive applications require high bandwidth and possibly QoS support. With CARD a suitable AR can be found. [6]

Finally, some terminology before we move on to discuss candidate access router discovery, its protocol functions, operational modes, security, target AR selection, and protocol messages.

**Mobile Node (MN)“**Mobile node is an IP host capable of moving its point of attachment to the Internet.” [4]

**Access Point (AP)“**A radio transceiver by which an MN obtains Layer 2 connectivity with the wired network.” [6]

**Access Router (AR)“**An IP router residing in an access network and connected to one or more APs. An AR offers IP connectivity to MN.” [6]

**Candidate Access Router (CAR)“**An AR to which MN has a choice of performing IP-level handoff. This means that MN has the right radio interface to connect to an AP that is served by this AR, as well as the coverage of this AR overlaps with that of the AR to which MN is currently attached.” [6]

**Target Access Router (TAR)“**An AR with which the procedures for the MN’s IP-level handoff are initiated.” [6]

**Capability“**A characteristic of the IP service offered by an AR that may be of interest to an MN when the AR is being considered as a handoff candidate.” [6]

**L2 ID“**Identifier of an AP, that uniquely identifies that AP.” [4]
2 Candidate Access Router Discovery Protocol Functions

CARD protocol consists of two functions: reverse address translation and discovery of CAR capability.

2.1 Reverse Address Translation

The MN listens to the L2 beacons to locate a new access point through which it can connect to a CAR. Reverse address translation is needed to map the AP’s L2 ID to the IP address of the CAR to which the AP is connected to. If the MN is able to establish a connection to CAR prior to handover decision CAR’s IP address can be easily obtained, for example, using RARP [2] in IPv4 networks. If establishing a new connection is not possible without breaking the IP connection to the current AR, the MN is not able to ask the IP address directly from the CAR. One solution for reverse address translation used in these cases is to use information cached to the MN. Another solution is to ask help from the current AR. [4]

In case the current AR’s help is used the MN sends the L2 ID of the candidate AP to the current AR, and expects it to resolve the IP address of the CAR. The current AR first checks its cache for L2 ID to IP address mapping. If there is no entry in the current AR’s mapping table the second step is to contact a CARD server. The CARD server holds the information about the L2 ID to IP address mappings belonging to its administrative domain. The CARD server then returns the IP address of the CAR to the current AR, which further returns it to the MN if needed. [4]

2.2 Discovery of Candidate Access Router Capability

Discovery of CAR capability makes it possible to choose such an AR that serves the MN’s needs best. Capability information is used as input to TAR selection algorithm. Issues related to TAR selection are discussed in chapter 3. Capabilities could be, for example, security functions, available bandwidth, access costs, and QoS services. The definitions of the capabilities are out of the scope of this document. It is also an open issue if there is going to be some limitation on the number of capabilities transferred between MNs and (C)ARs. [4, 6]

There are three ways to get capability information from CARs. First, such MN that can establish an IP connection with the CAR without breaking the connection to the current AR can ask capability information directly from the CAR. Second, MN’s can listen periodical transmissions on downlink broadcast channels, if the AP has decided to advertise its AR’s capabilities. Third, MNs ask help from the current AR. There are two phases in obtaining the CAR capabilities, when the MN has asked the current AR to help. First, the CARD server sends the CAR’s static capabilities. Then, the current AR enquires rest of the capabilities directly from the CAR. [4]
3 Target Access Router Selection and Capability Pre-filtering

Based on the capability information of CARs the new access router is selected. The selection is done with TAR selection algorithm. The algorithm itself is not part of CARD. The selection is invoked just before the handoff. [4]

TAR selection can be done either in the MN or in the current AR. Candidate Access Router Discovery Internet Draft [4] limits its view on performing TAR selection in the MN. When TAR selection is executed in the MN, the MN asks the capabilities directly from CARs or gets the capability information from the current AR. If TAR selection is located in the current AR, the MN sends its requirements to the current AR. Based on these requirements AR makes the TAR selection. [4]

When implementing TAR selection in the MN, a way to reduce over air traffic is capability pre-filtering. MN sends its preferences and the capability request to the current AR or to the CAR and receives a pre-filtered set of capabilities instead of the whole set. This approach is called downlink optimized. Situation when there is no prefiltering is called uplink optimized since instead of sending preferences and capability request the MN sends only the request. [4]

To reduce over air traffic even further context transfer framework may be utilized. The MN sends its preferences to the current AR, which, when AR changes, transfers the MN’s preferences to the new AR using context transfer framework. This way the MN does not need to send its preferences every time the AR changes. [4]

4 Security Considerations

CAR discovery, as many other protocols, is vulnerable to misuse when no security measures are taken. Here are some things that should be thought of.

There must be some way to authenticate the network elements. Security associations (SAs) are used for this purpose. Security association tells which set of security parameters is used in communication between a sender and a receiver [1]. With the help of SA, MN can be sure it is talking to a genuine AR and vice versa. CARD assumes that there always exists an SA between the MN and the current AR. SAs are also used between ARs to ensure the traffic between current AR and CARs. Also AR’s communication with CARD server is secured using SAs. The availability of SA is a requirement for secure transfer of capability information. It is not implicit that MNs and ARs have the necessary SAs, or even that they are able to establish the required SAs. [4]

Plain authentication might not be enough. Malicious nodes may find out AR’s IP address and capabilities by listening CAR discovery messages. This is such information that can be used, for example, to launch denial of service attacks or help in service hijacking. To make eavesdropping and attacks harder, CARD messages should be encrypted. Encryption is not only a positive thing. It increases computational load on CARs and MNs. Increased load leads to increased power consumption and thus shortens MNs’ operation time. [3, 6]

Not only malicious other nodes in the network may cause problems. Malicious mobile
node is also a risk to CARD. A MN can launch a denial of service attack by sending lots of requests to the ARs, the current AR or CARs. One can try to eliminate these attacks by limiting the number of requests accepted from a MN within a time period. A second solution is a scope ID. Scope ID gives a rough estimation of the coverage area of AR’s AP. This will help to detect whether the proposed CAR can really be a CAR, that is, the current AR and proposed CAR have overlapping coverage areas. Requests concerning false CARs can be ignored before the AR makes a capability request to the CAR. [4]

To improve CARD performance caching is needed at the AR. This means cache contamination is an issue. Cache contamination in CARD means having non-CAR entries in AR’s cache. These unnecessary entries bring down the hit ratio if cache size is not increased. And increasing the cache size is not a good solution. Lower hit ratio leads to more communication between AR and CARD server and thus slows down the protocol execution. Also, AR spends its processing power in capability exchange that will serve no-one. Two solutions are suggested to this: scope ID and soft state. Scope ID is explained in the previous chapter. Soft state means that information in the cache times out if the AR does not receive the same information from some other MN(s). [4]

5 Operational Modes of Candidate Access Router Discovery

CARD has two operational modes: MN orchestrated mode and network assisted mode.

5.1 Mobile Node Orchestrated Mode

In MN orchestrated mode the MN executes the CARD protocol, both reverse address translation and discovery of CAR capability. Use of MN orchestrated mode requires an IP connection from MN to CAR(s) without breaking the connection to the current AR. [4]

Figure 2 illustrates the function of MN orchestrated CARD. First, the MN discovers a new AP L2 ID by listening L2 beacons. Then, the MN establishes an IP connection with the new AP’s AR, the CAR. Next, the MN sends a request to the CAR asking CAR capabilities. The CAR replies with capability information. Then, the IP connection is closed. This procedure is repeated for every previously unknown access router. [4]

5.2 Network Assisted Mode

In network assisted mode CARD is executed in current the AR. The SA between the MN and the current AR is taken for granted. Trust between the current AR and CARD server or between the current AR and CAR is not so obvious. This trust relationship must be established by using SAs to guarantee secure reverse address translation and capability transfer. [4]

Figure 3 illustrates the function of network assisted CARD. If capability pre-filtering is used the MN sends its preferences to the current AR. After hearing a new AP beacon the MN sends the L2 ID to the current AR for reverse address translation. The current AR first checks its cache. If the L2 ID to IP address mapping is not available in the cache the
current AR sends a request containing the L2 ID to the CARD server. Next, the CARD server replies with the CAR’s IP address and static capabilities. Then, the current AR sends a capability request to the CAR, which replies with its capabilities. Last, the current AR sends the pre-filtered capabilities and the IP address to the MN for TAR selection. The procedure is repeated from hearing a beacon onwards for every new AP. The current AR caches the L2 ID to IP address mappings and the capabilities, so, when the same AP is requested again there is no need to contact the CARD server or the CAR again. [4]

6 Candidate Access Router Discovery Protocol Messages

CARD protocol is initiated when the MN discovers a new AP while listening L2 beacons. The format of the messages depends on the interface over which the messages are sent. MN-AR interface uses ICMP messages. The protocol messages are sent in separate Internet Control Message Protocol (ICMP) messages or piggybacked on other ICMP messages. Interfaces AR-AR and AR-CARD server use User Datagram Protocol (UDP) as transport mechanism. [4]

All interfaces use options CARD request and CARD reply. In addition to these requests AR-CARD server interface has two more options: CARD registration request and CARD registration reply. Registration messages are used to update CARD server when a CAR is initialized and later when AP status or CAR capabilities change. CARD request and reply perform the actual CARD protocol, reverse address translation and discovery of CAR capability. [4]

Options on MN-AR interface have fields type, length, flags, and sequence number. Type tells whether the option is a request or reply, length is used for indicating the total length of the option including sub-options. One bit of the flags field is reserved for indicating the piggybacking capability of the sender, rest of the flags bits are reserved and initialized to 0. Sequence number is used to link replies to requests. The format of the option is clarified in figure 4. [4]
7 Thoughts about the Candidate Access Router Discovery

Here are some questions the Internet Drafts about candidate access router discovery did not answer. Also, the advantages and disadvantages of operational modes of CARD and the location of TAR selection are discussed.
Discussion about reverse address translation in Candidate Access Router Internet Draft [4] is limited to APs and CARs that are in the same administrative domain as the current AR. In such situations the CARD server is able to do the reverse address translation. It is unclear how the address translation is continued if the CARD server does not know the AP because the AP is under different administrative domain. To get the address translation done the CARD server presumably continues the address translation by contacting CARD servers in other administrative domains. It should be considered how to verify that the responses come from authorized CARD servers. Additionally, it should be decided whether the CARD servers caches the information received from other CARD server or not, and if cached, for how long.

Security association establishment is demanded only for AR-AR and AR-CARD server communications. SA between the MN and the current AR is considered implicit. [4] To execute MN orchestrated CARD securely there should also be an SA available between the MN and CAR, either pre-established or established on demand.

Then some remarks on operational modes of CARD. MN orchestrated mode sets more requirements on MN battery power and processing capabilities since the MN contacts the CARs directly. Also, MN orchestrated mode causes more load on CARs. MNs under the same AR contact the CAR separately. In network assisted mode the CAR would be

<table>
<thead>
<tr>
<th>sub-option</th>
<th>MN-AR</th>
<th>AR-MN</th>
<th>AR-CAR</th>
<th>CAR-AR</th>
<th>AR-CARD server</th>
<th>CARD server-AR</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2 ID</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>preferences</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>requirements</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>capability container</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>lifetime</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
contacted only once by the current AR, assuming the cache entry has not timed out. In addition, in MN orchestrated mode the CAR has to send its static and dynamic capabilities to the MNs. In network assisted mode it is enough for the CAR to send its dynamic capabilities on request since the static capabilities are delivered through CARD server. If there is a need to reduce over air traffic the network assisted mode with TAR selection in the AR is a good solution. The number of the MNs can help to judge will the MN orchestrated mode cause too much load or are the CARs able to handle the direct requests. Also, the current AR could be overloaded trying to serve many MNs finding several new APs.

Even though Candidate Access Router Discovery Internet Draft [4] limits its view on executing TAR selection in the MN, I’ll now discuss pros and cons of TAR selection both in the MN and in the AR. Executing the TAR selection in the MN means sending the capabilities over air from the current AR or the CAR to the MN. This may cause large capability traffic. Over air traffic decreases significantly if TAR selection is executed in the AR. Then, only MN’s requirements, discovered APs’ L2 ID’s and the chosen TAR’s IP address need to be sent over air. The AR has to remember which APs a MN has reported and execute the TAR selection based on that information. There is a risk that when the AR executes the TAR selection the MN no longer is in the coverage area of the CAR that is chosen as TAR. After the TAR selection the AR informs the MN about the TAR. At this point the MN should be able to notice somehow that the chosen TAR is out of its reach and ask for a new TAR from the AR. If the TAR selection is executed in the MN there is no such risk. In situations when the there are two or more CARs with the same capabilities the MN is the only one that can choose the best CAR. The decision is based on signal strength of AP beacons. The stronger the signal the better choice the CAR is likely to be. To sum up one could say the TAR selection in the MN is good in taking into consideration the MN’s changing situation. Whereas the TAR selection in the AR reduces over air traffic and saves the MN’s battery power and computational capacity for other things. Of course, the place for TAR selection can be chosen only when using network assisted mode.

How does the AR handle situations when the MN discovers several APs that belong to the same CAR, or two or more MNs discover separate APs belonging to the same CAR? Does the AR request address translation for each AP separately? Or does the CARD server inform the current AR about all APs belonging to the CAR when resolving the L2 ID of one of the APs. The capabilities are per CAR, so asking same capabilities separately from the CARD server for every AP belonging to a certain CAR seems as a waste of resources. On the other hand storing L2 IDs in the AR for those APs that no MN has asked for can also be considered inefficient. The AR CARD server interface is not the only place where this problem arises. The MN asking the information about a new AP belonging under the same CAR as some other AP the MN previously found receives the same CAR IP address and capabilities again. For MN-AR interface the problem of sending same capabilities several times, each time because of a new AP, is not as big problem as for AR-CARD server interface because one MN is not so likely to find several APs belonging under the same CAR compared to all the MNs the AR is serving.

This document concentrates on CARD using a server for reverse address translation and handling static capabilities. Also serverless approach for CARD has been proposed. In Dynamic Protocol for Candidate Access Router Discovery [5] the AR queries the CARs directly, but also updates its cache when a MN hands over to it. The new AR updates into
its cache the L2 ID and IP address of the MN’s previous point of attachment. Consequently, ARs learn about their geographical neighbor ARs bi-directionally, not only when handing over a MN, like in CARD, but also when receiving a MN as a result of handover.

Candidate access router discovery is one solution to the problem: how to find the next router to connect to. There are still many open questions, some of them discussed in this chapter. Some seamless handover mechanisms proposed assume that the new access router is known when the handover is initiated. CARD is one way of locating the candidate routers. The future of CARD depends greatly on the evolution of seamless handover mechanisms, and on how the open issues of CARD are solved.

References


